1. A method for securely storing a public key for encryption of data in a computing device, the method using a user-specific key pair which is securely stored in the computing device, the method comprising:

a receiving step of receiving a target public key corresponding to a target device;

an obtaining step of obtaining a user-specific key pair from a secure registry;

a key encrypting step of using a user-specific private key from the user-specific key pair to create a target key verifier based on the target public key;

a storing step of storing the target key verifier and the target public key in a storage area;

a retrieving step of retrieving the target key verifier and the target public key from the storage area;

a verification step of applying a user-specific public key from the user-specific key pair to the target key verifier for verifying the authenticity of the target public key; and

a data encrypting step of encrypting data with the target public key, in the case that the authenticity of the target public key is verified, thereby creating encrypted data for transmission to the target device.

2. A method according to Claim 1, wherein the user-specific key pair is obtained from a key function call which is supported by an operating system executing in the computing device.

3. A method according to Claim 2, wherein the operating system securely maintains a user-specific key pair for each of a plurality of users of the computing device.

4. A method according to Claim 3, wherein each user-specific key pair can only be accessed by providing the operating system with user identification data corresponding to the user-specific key pair.

a1

5. A method according to Claim 1, wherein the target key verifier created in the key encrypting step is an encrypted version of the target public key.

6. (Canceled).

7. A method according to Claim 5, wherein the verification step includes decrypting the target key verifier with the user-specific public key using a decryption algorithm.

8. A method according to Claim 7, wherein the verification step further includes using a key verification algorithm to compare the decrypted target key verifier to the target public key for verifying the authenticity of the target public key.

9. A method according to Claim 8, wherein the verification step is performed by a verification function call which is supported by an operating system executing in the computing device.

10. A method according to Claim 1, wherein the target key verifier created in the key encrypting step is a digital signature of the target public key.

a1

11. A method according to Claim 10, wherein the digital signature of the target public key is created by applying a hashing algorithm to the target public key to obtain a target key hash, and then encrypting the target key hash with the user-specific private key using an encryption algorithm.

12. A method according to Claim 10, wherein the digital signature of the target public key is created by applying a hashing algorithm to the target public key to obtain a target key hash, and then subjecting the target key hash to a security algorithm.

13. A method according to Claim 12, wherein the verification step includes decrypting the target key verifier with the user-specific public key using a decryption algorithm to obtain a decrypted target key hash.

14. A method according to Claim 13, wherein the verification step further includes reapplying a hashing algorithm to the target public key to obtain a new target key hash and using a hash verification algorithm to compare the decrypted target key hash to the new target key hash for verifying the authenticity of the target public key.

a'

15. A method according to Claim 14, wherein the verification step is performed by a verification function call which is supported by an operating system executing in the computing device.

16. A method according to Claim 1, wherein the receiving step includes applying a hashing algorithm to the received target public key to obtain a received target key hash and using a hash verification algorithm to compare the received target key hash to a test target key hash for verifying the authenticity of the received target public key.

17. A method according to Claim 16, wherein the test target key hash is input by a user.

18. A method according to Claim 17, wherein the target device is a printer and wherein the test target key hash is obtained from a test page printed by the printer.

19. A method according to Claim 1, wherein the target device is a printer and the target public key is a printer public key.

20. A method according to Claim 19, wherein, in the receiving step, the printer public key is received in response to a key request sent to the printer.

a1

21. A method according to Claim 19, wherein the method is performed in a printer driver executing on the computing device.

22. A method for securely storing a printer public key for encryption of print data in a computing device, the method using a user-specific key pair which is securely stored in the computing device, the method comprising:

a receiving step of receiving a printer public key corresponding to a printer;

an obtaining step of obtaining a user-specific key pair from a secure registry upon receipt of a corresponding user identification;

a first hashing step of applying a hashing algorithm to the printer public key to create a first printer key hash;

an encryption step of applying an encryption algorithm to encrypt the first printer key hash with a user-specific private key from the user-specific key pair, thereby creating a printer key signature;

a storing step of storing the printer key signature and the printer public key in a storage area;

a retrieving step of retrieving the printer key signature and the printer public key from the storage area;

a second hashing step of applying the hashing algorithm to the retrieved printer public key to create a second printer key hash;

a decrypting step of applying a decryption algorithm to decrypt the printer key signature with a user-specific public key from the user-specific key pair, thereby retrieving the first printer key hash;

a verification step of applying a verification algorithm to compare the first printer key hash with the second printer key hash, for verifying the authenticity of the retrieved printer public key; and

a print data encrypting step of applying an encryption algorithm to print data using the retrieved printer public key, in the case that the authenticity of the retrieved printer public key is verified, to create encrypted print data for transmission to the printer.

23. A method for authentication of a printer public key received by a computing device, the method comprising:

a first receiving step of receiving in the computing device a printer public key corresponding to a printer;

a hashing step of applying a hashing algorithm to the printer public key to create a first printer key hash;

a second receiving step of receiving in the computing device a predetermined second printer key hash obtained from a test page printed by the printer, wherein the second printer key hash is input into the computing device by a user-input means connected to the computing device;

a verification step of applying a verification algorithm to compare the first printer key hash with the second printer key hash, for verifying the authenticity of the received printer public key; and

a storing step of storing, in the case that the authenticity of the received printer public key is verified in the verification step, the received printer public key in a memory area of the computing device.

24. A computing device for authenticating a public key for encryption of data, said computing device comprising:

a program memory for storing process steps executable to perform a method according to any of Claims 1 to 23; and

a processor for executing the process steps stored in said program memory.

25. Computer-executable process steps stored on a computer readable medium, said computer-executable process steps for authenticating a public key for encryption of data, said computer-executable process steps comprising process steps executable to perform a method according to any of Claims 1 to 23.

a1

26. A computer-readable medium which stores computer-executable process steps, the computer-executable process steps to authenticate a public key for encryption of data, said computer-executable process steps comprising process steps executable to perform a method according to any of Claims 1 to 23.

27. (New) An information apparatus which transmits encrypted data to a target device, the information apparatus securely storing a public key for encryption of the data and utilizing a user-specific key pair which is securely stored in the apparatus, comprising:

receiving means for receiving a target public key corresponding to a target device;

obtaining means for obtaining a user-specific key pair from a secure registry;

key encrypting means for using a user-specific private key from the user-specific key pair to create a target key verifier based on the target public key;

storing means for storing the target key verifier and the target public key;

retrieving means for retrieving the target key verifier and the target public key from the storage means;

verification means for applying a user-specific public key from the user-specific key pair to the target key verifier for verifying the authenticity of the target public key; and

a'

data encrypting means for encrypting data with the target public key, in the case that the authenticity of the target public key is verified, thereby creating encrypted data for transmission to the target device.

28. (New) An information apparatus which transfers encrypted print data to a printer, the apparatus comprising:

retrieving means for retrieving a public key from said printer;

generating means for generating verification information from the public key;

recognizing means for recognizing a printing instruction;

verification means for verifying, in response to the recognition of the printing instruction, that the public key is not changed from the retrieved public key; and

control means for controlling encryption processing which is performed by using said public key when the retrieved public key is verified as unchanged, and which is not performed when the retrieved public key is verified as changed.

29. (New) An information apparatus according to Claim 28, further comprising:

obtaining means for obtaining a user specific key stored in a computer;

input means for inputting authentication information; and

determining means for determining whether to allow the obtaining means to obtain the user specific key.

a1

30. (New) An information apparatus according to Claim 28, wherein said control means controls the encryption processing to encrypt the print data by using a user specific key obtained by an obtaining means and to encrypt the user specific key by using the public key.

31. (New) An information processing method for transferring encrypted print data to a printer, the method comprising:

a retrieving step of retrieving a public key from said printer;

a generating step of generating verification information from the public key;

a recognizing step of recognizing a printing instruction;

a verification step of verifying, in response to the recognition of the printing instruction, that the public key is not changed from the retrieved public key; and

a control step of controlling encryption processing which is performed by using said public key when the retrieved public key is verified as unchanged, and which is not performed when the retrieved public key is verified as changed.

32. (New) An information processing method according to Claim 31, further comprising:

an obtaining step of obtaining a user specific key stored in a computer;

an input step of inputting authentication information; and

a determining step of determining whether to allow the obtaining step to obtain the user specific key.

33. (New) An information processing method according to Claim 31, wherein said control step controls the encryption processing to encrypt the print data by using a user specific key obtained by an obtaining step and to encrypt the user specific key by using the public key.